REMARKS

Claims 8 to 14 were canceled. New claims 20 to 30 were added. Claims 15 and 18 were amended. No new matter has been added.

Claims 15 to 30 are now pending. Applicants respectfully request reconsideration of the present application in view of this Amendment Response.

35 U.S.C. §112, first paragraph

Claims 8, 15, and 18, were rejected under 35 U.S.C. §112, first paragraph, for lack of enablement. Applicants respectfully submit that the Specification is clear and enabling in its description of how to make and how to use embodiments of the present invention. For example, pages 5 through 9 describe various embodiments of the present invention. Thus, Applicants have amended the claims in order to clarify the claim language. Claim 8 has been canceled. Accordingly, Applicants respectfully submit that claims 15 and 18, as well as new independent claim 20, as presented satisfy the enablement requirement, and withdrawal of the rejection under 35 U.S.C. §112, first paragraph, is respectfully requested.

35 U.S.C. §103

In the earlier final Office Action, claims 8 to 18 were rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 5,805,204 to Thompson ("Thompson reference") in view of U.S. Patent No. 6,285,991 to Powar ("Powar reference") and further in view of U.S. Patent No. 6,169,805 ("Dunn reference").

Claims 8 to 14 were canceled, thus, the rejection of those claims is moot.

Applicants respectfully submit that amended claims 15 to 18 are allowable over the cited Thompson, Powar, and Dunn references.

The Thompson reference refers to an interactive video guide in which object code is transmitted to set-top decoder units located in customers' homes. The Thompson reference appears to indicate that to send encrypted data, a random number is first generated by a program within the headend computer; and an appropriate imbedded key (the chosen key for the time period) is selected and loaded into the system specific algorithm. Apparently, the random number is encrypted using the DES algorithm which has been initialized and loaded with the appropriate key, producing a result which is the current system seed key. The seed key is then loaded into the system specific algorithm through which the actual transmitted data is passed. The initial random number is transmitted in clear text along with the encrypted data. When the data is received by a subscriber unit, a period identifier may be used to identify which of the keys

previously and securely imbedded into the smart card will be used for the decryption process. This key must be the same one used at the headend computer for the same time period.

The Powar reference refers to an interactive electronic account statement delivery system for using over the Internet. Specifically, the Powar reference refers to a system where the certification authority grants digital certificates to the certificated banks, which in turn grant digital certificates to billers and customers. Then, digital certificates form the basis for encryption and authentication of network communications, using public and private keys. The reference refers to the certificates as being stored as digital data on storage media of a customer's or biller's computer system, or contained in integrated circuit or chip cards physically issued to billers and customers.

The Dunn reference refers to secure communications over a network such as the Internet such that a sender prepares a file containing confidential information and downloads encryption/decryption software from a URL location on the Internet. A key for decrypting the file is obtained by a user through an HTML page which requests the Key which a receiver enters. The file is then downloaded and decrypted using the key K.

In contrast, claim 18, for example, is directed to an encryption system, including a secret key having a defined key length; a variable parameter having a length which is a function of the defined key length; a symmetrical cipher; a Vernam key having a length that is equal to a length of a message to be protected; ***the Vernam key being generated from the symmetrical cipher encryption of the secret key and the variable parameter,*** the Vernam key encrypting the message using logic operations from a Vernam cipher; at least one of a message-transmission path and a secure channel, the message-transmission path being a path over which the encrypted message is communicated, ***the secure channel being secured by encrypting the secret key and the variable parameter with an asymmetrical cipher, the secure channel being separate from the message-transmission path; and a crypto-module including a storage space and one of the symmetrical cipher and the asymmetrical cipher, wherein the crypto-module is separate from the encryptor, the storage space is used to store the Vernam key,*** and any Vernam cipher operations are performed in the encryptor, wherein the secret key and the variable parameter are communicated over at least one of the message-transmission path and the secure channel and, subsequently, used in regenerating the Vernam key, the regenerated Vernam key decrypting the message.

None of the references, alone or in combination, appear to teach or describe such a system in which a secret key and a variable parameter are devised in the manner described, e.g., as in claims 15, 18, and 20, and then transmitted via a secure channel separate from a message-transmission path. Further, none, alone or in combination, appear to teach or describe a system and method which can use the same Vernam cipher, but still have a robust system in that the

Vernam key is used and then discarded after use. Further, none, alone or in combination, appear to regenerate a Vernam key from an encrypted transmitted secret key and variable parameter. Further, none, alone or in combination, appear to teach or describe using a separate storage space to store a plurality of generated Vernam keys to be used with the Vernam cipher, the use of stored information being useful in reducing the transmission time and needed resources of an encrypted message.

Accordingly, Applicants respectfully submit that the Thompson, Powar, and Dunn references in combination or alone do not teach or describe all of the features of claim 18. Allowance of claim 18 is respectfully requested.

Claims 15 and dependent claims 16 to 17 and 19, recite features analogous to those of claim 18, and should be allowable for essentially the same reasons as claim 18.

Accordingly, Applicants respectfully request the withdrawal of the rejection of claims 15 to 18 under 35 U.S.C. § 103(a). Applicants further submit that new claims 20 to 30 recite features analogous to those of claim 15, and are believed allowable for at least the same reasons as claim 15.

CONCLUSION

For at least the foregoing reasons, Applicants respectfully submit that any outstanding rejections of claims 15 to 19 under 35 U.S.C. §§ 103(a), 112 have been overcome, and that all pending claims 15 to 30 are in condition for allowance.

It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

Respectfully submitted,

Dated: April 13, 2010

By: /Linda Lecomte/
Linda Shudy Lecomte (Reg. No. 47,084)

CUSTOMER NO. 26646

KENYON & KENYON LLP
One Broadway
New York, New York 10004
(212) 425-7200